Participation Handbook

Cyber Resilience Tabletop Exercise (TTX)

ICAO Middle East Region

Exercise Overview

Exercise Name: Cyber Resilience Tabletop Exercise
Exercise Date: *13-16 November 2022*
Location: Fairmont Hotel, Amman, Jordan.
Hosted by: *Jordan Civil Aviation Regulatory Commission (CARC)*

Exercise Objectives:

- **Develop awareness and promote a common understanding of cyber vulnerabilities, and resultant risks affecting the air navigation system.** For example:
    - Identify cyber interdependences of infrastructure and real-world economic and political scenarios
    - Raise awareness of the economic and safety impacts associated with a significant cyber incident

- **Identify gaps in State policies and operations.** For example:
    - Identify policies/issues that hinder or support cyber requirements
    - Identify communication paths and levels of coordination to improve cyber incident response and recovery, as well as identify critical information-sharing paths and mechanisms
    - Identify, improve, and promote public and private sector interaction in processes and procedures for communicating appropriate information to key stakeholders and the public

- **Empower participants with measures to mitigate the exploitation of critical Air Navigation systems by identifying and promoting mechanisms for information sharing .** For example:
    - Examine the capabilities to prepare for and respond to the effects of cyber-events
    - Discuss leadership decision-making and local/regional/international coordination of cyber-event responses in accordance with any existing plans.
    - Validate information-sharing relationships and communications paths for the collection and dissemination of cyber incident situational awareness, response, and recovery information
    - Exercise inter-governmental coordination and incident response

- **Introduce International Aviation Trust Framework (IATF) and promote global benefits for the aviation Ecosystem by being part of the (IATF).**

Exercise Themes:

- **Expectations, skills & experience**

    - Role, responsibilities, authorities & interactions with others
- **Policies and procedures**
    - Current plans and procedures & significant inconsistencies, if any
- **Risks to the safety of flight operations**
    - Hazards, & vulnerabilities that could be impactful
- **Role of International Aviation Trust Framework.**

Table Top Exercise Focus Area (Scope)

- ***Trusted information exchange***
    - Identified parties
    - Information Management: confidentiality, integrity, and availability of data
        - Flight planning systems
        - Airport systems
        - Communication systems
        - Operational network segmentation
    - Cyber hygiene across entities
        - Policies, practices and procedures
        - Information Security Framework
    - Regional network management
        - Network monitoring
        - Incident management

Point of Contact:

- *Alnadaf, Muna, REGIONAL OFFICER, COMMUNICATIONS, NAVIGATION AND SURVEILLANCE, OSG/MID.* malnadaf@icao.int

Facilitators:

- *Goodfellow, Michael, TECHNICAL OFFICER, GLOBAL INTEROPERABLE SYSTEMS, ANB/AN/GIS.* MGoodfellow@icao.int
- *Kornetskiy, Anton, TECHNICAL OFFICER, GLOBAL INTEROPERABLE SYSTEMS, ANB/AN/GIS.* AKornetskiy@icao.int

Preliminary Exercise Schedule

DAY 1 (13 NOVEMBER 2022)		
Time	**Activity**	**Speaker/Moderator**
0800 - 0900	Registration	
0900 - 0930	Opening Session	Jordan CARC ICAO RO
0930 - 1000	Introduction	ICAO HQ
1000 - 1030	*Coffee Break*	
1030 - 1045	The regional perspective and activities	ICAO RO
1045 - 1115	Setting the cyber scene	ICAO HQ

1115 - 1200	TTX exercise introduction	All
1200 - 1230	*Coffee Break*	
1230 - 1400	TTX exercise: Scenario 1	All
1400 - 1430	Celebration on International ATSEP day	All
1430	Lunch	
DAY 2 (14 NOVEMBER 2022)		
0900 – 0930	Summary of the previous day work	ICAO HQ
0930 - 1030	TTX exercise: Scenario 1 (to be cont'ed)	All
1030 - 1100	*Coffee Break*	
1100 - 1230	TTX exercise: Scenario 2	All
1230 - 1300	*Coffee Break*	
1300 - 1430	TTX exercise: Scenario 3	All
1430	*Lunch*	
DAY 3 (15 NOVEMBER 2019)		
0900 - 1030	TTX exercise: Scenario 3 (to be cont'ed)	All
1030 - 1100	*Coffee Break*	
1100 – 1230	International Aviation Trust Framework - Facilitated Discussion	ICAO HQ
1230 – 1300	*Coffee Break*	*Coffee Break*
1300 - 1400	Review of TTX, lessons learned and round-table Q&A	All
1400	*Lunch*	

Terms and Definitions

The terms and definitions herein are specific to this exercise and may differ from those presented in other ICAO documents. They are purely to clarify the terms in the context of these exercises.

Aviation-related:

- ***Aviation Domain V. Aviation Ecosystem***
  - **Aviation Domain:** The global airspace, including domestic, international, and foreign airspace, as well as all manned and unmanned aircraft operating in that airspace, and people and cargo present in that airspace, and all aviation-related infrastructures.
  - **Aviation Ecosystem**: An extensive multi-layered network of intersection elements with integral roles in the Aviation Domain and involves six primary entities: Airports, Airlines, Airlift, Aircraft, Actors, and Aviation Management.
- **Other Aviation Terms and Definitions**
  - **ANSP**: Used generically for all air navigation service providers
  - **Airline**: Used generically for all flagged air carriers (passengers, cargo)
  - **AIRAC**: Aeronautical Information Regulation and Control synchronization process
- **Communications Networks**: Responsible for the circuits, networks, and equipment supporting voice and data (email, surveillance, flight plans, etc.)
- **Executive Stakeholders**: Senior leadership responsible for making policy, "non-routine" decisions.

- **Operations Stakeholders**: Provide air traffic control and traffic flow, responsible for making "routine" decisions based on existing policy and procedures.
- **International Aviation Trust Framework (IATF)** is a set of policies, requirements and best practices that will enable trusted, resilient and secured ground-ground, air-ground, and air-air exchange of digital information among all current and prospective aviation stakeholders
- **Unmanned aircraft system (UAS)**: An aircraft and its associated elements which are operated with no pilot on board.
    - *Discussion will feature a small drone (251 g -25 kg) equipped with a professional DSLR quality camera
- **State of Registry**. The State on whose register the aircraft is entered.
    - All unmanned aircraft (UA) should be registered according to part 101 of ICAO Model UAS Regulations.
- **Remote pilot**. A person charged by the operator with duties essential to the operation of a remotely piloted aircraft and who manipulates the flight controls, as appropriate, during flight time.
- **Drone pilot license.** Drone pilots must carry a valid drone pilot certificate at all times while operating their drone.

Cyber-related

- **Cyber Hygiene:** Practices and steps to maintain computers and devices system health and improve online security.
- **Distributed Denial of Service:** A denial of service technique that uses numerous systems simultaneously to impair the authorized use of information system resources or services, typically by flooding the network with packets of huge amounts of data.
- **Malware:** Software that compromises the operation of a system by performing an unauthorized function or process.
- Phishing: A digital form of social engineering to deceive individuals into providing sensitive information.
- **Spoofing:** Faking the sending address of a transmission to gain illegal [unauthorized] entry into a system; the deliberate inducement of a user or resource to take incorrect action. Note: Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing.

IATF Facilitated discussion terminology

Exercise structure

- **Facilitated Discussion:**
    - Players are encouraged to actively interact in accordance with their real-world actions, responsibilities, policy, and expertise.
    - Players are encouraged to respond to the scenario using their knowledge of current plans, capabilities, and insights.

- **TTX**:
    - The moderators will present the situation and players will engage in a discussion of appropriate response actions and issues that arise from the scenario at hand.

- The situation will have a number of injected parameters throughout the narrative. The goal of the injections is to change one or more variables in the presented situation or to advance the story.
- The scenario will conclude when the storyline is finished or when the objectives of the situation have been met.
- The next situation will then be introduced (as applicable). Subsequent situations may build upon previous situations or may be completely unrelated.

Participant's roles and responsibilities

The term participant encompasses many groups of people, not just those playing in the exercise. At a minimum, a Moderator and Players are required. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

- **Moderator**: Directs the overall flow during the conduct of the exercise.
- **Subject Matter Experts (SME):** As requested, assist by providing relevant information, analysis, and recommendation in their area of expertise or providing subject matter expertise.
- **Players:** Active in discussing or performing their regular roles and responsibilities during the exercise.
- **Recorders**: Monitor the overall flow of exercise & help document actions and decisions, in support of post-exercise information/documents.
- **Observers:** Observe the overall flow of the exercise in a manner that does not directly affect its conduct.

Participation Guidelines

The Cyber Resilience TTX scenario will be based on **Flight Plan Management process** and presented in three parts (3 scenarios plus several injects). The intent of these injects is to highlight the interconnectedness of cyber systems with physical infrastructure and to exercise coordination and communication between stakeholders. Following each part, players will have a set time to review the module and debate the discussion questions.

IATF Facilitated discussion scenario will be based on the safety of UAS operations internationally and domestically. It will be presented in 2 parts plus several injects. The intent of these injects is to highlight global benefits for the aviation Ecosystem by being part of the International Aviation Trust Framework**.**

Players have no advanced knowledge of the scenarios and will receive all information at the same time. Although based on a plausible scenario, this TTX is not intended to replicate a real attack or simulate a full response; the goal is to examine and debate incident coordination and communications issues rather than determine a "best" response.

Although general terms are used in the scenario, players should emerge themselves in the exercise as if this is happening in their region and in their airspace. Players should always note that the scenario presented is fictitious and any names mentioned are only used for context or as examples. Players should also note that the scenarios presented are based on certain assumptions that might be different from their own State or region. If this is the case, please feel free to point out the differences and discuss them.

This exercise will be held in an open, low-stress, no-fault environment. Varying viewpoints, even disagreements, are expected and even encouraged.

During the TTX and IATF facilitated discussion:

- Respond to the scenario using your own knowledge of current plans, policies, and capabilities (i.e., you may use only existing assets) and insights. No other resources are required for players to actively participate in the TTX.
- Think outside the box. There is no right or wrong answer. Players are strongly encouraged to participate in in-depth discussions, as the primary purpose of the exercise is to exchange knowledge and share experiences between players.
- Discuss and present multiple options and possible solutions. Decisions are not precedent-setting and may not reflect your final position on a given issue.
- Identify issues but also suggest and recommend actions that could improve cyber efforts. Problem-solving efforts should be the focus.

There should not be the dissemination of exercise materials or discussion; *communication should remain in-room*. The outcomes of the discussion will be distributed to all participants and observers and may be freely shared. No State, organization, or person will be directly attributed to the discussion outcomes.

Cyber Resilience TTX scenario has three major adversarial objectives:

- To disrupt specifically targeted systems through cyber events (critical or otherwise)
- To compromise systems for financial gain
- To undermine public confidence in air travel